WHITE PAPER

AMERICAN WATER

Maureen Duffy
T: 856-309-4546
maureen.duffy@amwater.com

Cybersecurity Threats at Water and Wastewater Utilities

Introduction

Until recently, water utilities regarded resiliency as a matter of defense against severe weather events. Now, the threat of cybersecurity breaches has emerged as a growing risk for the critical infrastructure sector. And as utilities, whether water, electric, gas or telecom, each one has a deep responsibility to provide vital services to customers.

Critical infrastructure systems including water and wastewater utilities are increasingly under attack – they are the target of sophisticated cyber criminals, terrorists and hostile nation states attempting to access and disrupt the nation's essential services systems. Over the past decade, utilities have leveraged advanced communications systems and the "Internet-of-Things" to deliver better, safer, more reliable and more efficient service to customers. However, with these benefits come increased risks.

As recently as October 2017, the U.S. Department of Homeland Security and the Federal Bureau of Investigation issued a joint warning that details the "advanced persistent threat" to various targets, including utilities.[1] It is not a question of if our critical infrastructure will be targeted, but when and to what extent.

According to a *USA TODAY* analysis of federal energy records, about once every four days, part of the nation's power grid — a system whose failure could leave millions in the dark — is struck by a cyber or physical attack.[2]

While electric, gas and telecom services are also critical to health -- such as the electricity to run medical equipment or digital communications to manage challenging situations -- none is as directly key to human health as the provision of clean and safe water that is ingested by the people we all serve, or the provision of basic sanitation services to avoid diseases.

Add to that, these utility systems are more and more intertwined--energy production requires tremendous amounts of water; water treatment and delivery requires access to significant amounts of uninterrupted electricity; and advanced communications services form the foundation of smarter utility grids and customer interfaces.

Threats

Cybersecurity

According to the Department of Homeland Security, there are about 160,000 public water systems and more than 16,000 public wastewater systems in the United States. These systems continue to advance the use and integration of connected technology driving a concern about cybersecurity threats.

[1] U.S. Department of Homeland Security. https://www.us-cert.gov/ncas/alerts/TA17-293A.
[2] USA TODAY. "Bracing for a big power grid attack" 'One is too many". March 24, 2015.

The critical nature of a utility's infrastructure makes it a prime target for cyberattacks. Cybersecurity threats are an ever-present challenge that utilities must learn to defend against and minimize. Generally, the utilities sector – including the water and wastewater, is a frequent target of attack. These attacks, if undetected, can result in service interruptions, data theft, and infrastructure damage. Cyberattacks on the nation's water supply and water quality infrastructure could result in disruption of critical water and wastewater service, and impacts to public health and the environment.

In August 2017, the President's National Infrastructure Advisory Council (NIAC) unanimously approved a 45-page report that found the federal government and the private sector are "falling short" in protecting critical systems.[3]

American Water recognizes the essentiality of its water and wastewater services, and acknowledges the severity of cyber threats. The company has always endorsed a "safety and security approach" to water and wastewater operations, and this persistence extends to cyber threats as well.

Black Sky Events

The term "Black Sky" is quickly becoming a term of art for preparedness. Traditionally, Black Sky referred to a widespread, long-duration power outage. Such extreme disruptions can stem from extreme weather events, natural disasters or man-made attacks on critical infrastructure like the electric grid.

The water sector is also subject to the threat of severe systemic disruptions as a result of natural disasters or man-made attacks. The interconnected nature of 21st century utility systems amplifies these threats.

In fact, about four years ago, the Electric Infrastructure Security Council (EIS) began working with electric utilities, DHS and DoD, along with the UK and Israel, on a plan to address a widespread and long duration power grid outage. In preparing the first handbook for the electric sector, they quickly realized that one of the most pressing health challenges of such a massive outage would actually be water related--the potential lack of drinking water, basic sanitation, and fire protection. The most recently released handbook in fact was focused on those issues.[4]

The connectivity among utilities as well as the increasing use of new technologies by utilities offers tremendous promise, but also highlights many distinct risks. Black Sky events are among the most important because they can be so devastating.

One key finding of the Black Sky effort is that extended and widespread loss of water or wastewater service for could cause unplanned mass evacuations, which would be chaotic, unmanageable. Therefore, the goal is that utilities partner with local and state emergency planners to avoid the "tipping point," and enable the largest possible number of customers to remain in their homes for as long as possible. Resource priority, outage information and critical facilities are part of those partnering discussions.

[3] U.S. Department of Homeland Security. The National Infrastructure Advisory Council.

[4] The EPRO Handbook Series. Consensus-based, cost effective strategies and best practices for Black Sky Hazard resilience and whole community response. An evolving, collaborative, peer-reviewed resource for utilities and their government and NGO partners.

Resiliency

As the nation's largest water and wastewater utility, touching over 12 million customers in 16 states, American Water is investing in intelligent infrastructure, advanced IT networks, cloud-based platforms, and newer SCADA systems to provide safe, efficient, and reliable service.

While technology systems are potentially prone to cyberattacks, they also enable us to be more reliable, efficient, and resilient. These technologies are used in developing an intelligent water system to do things such as protect water supplies; detect leaks; enhance internal efficiencies; and recover more quickly from service disruptions. Additionally, these technology systems are used to communicate with customers and enhance interactions.

According to the American Water Works Association (AWWA) in a 2014 resolution, “Every public water supply and wastewater utility should assess the likelihood and consequences of a supply disruption, identify critical vulnerabilities, and consider alternative power or supply redundancy to mitigate service disruptions lasting up to 72 hours or longer if public health, environmental, or economic impacts are severe.”

Advanced communications networks are an increasingly integral component of operations and services. Technology creates a number of benefits and efficiencies but also acts as a vector for cyberattacks. As information technology becomes a pervasive and ubiquitous part of water service, the vectors for attack might inevitably increase.

As we advance technology, American Water is building cybersecurity protocols into almost every aspect of its business**.** Diligence is key to ensuring security controls are foundational to the implementation and operation of new technology systems whether they are cloud-based or in house.

National Institute of Standards and Technology

American Water’s security program is consistent with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), created because of a 2013 executive order from President Obama to improve critical infrastructure. The Framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk. The framework is voluntary for the water sector at this point.

The AWWA subsequently released the Process Control System Security Guidance document to support water utility adoption of the framework. American Water participated as a subject matter expert on the development of that document. The document details 12 steps the water utility industry should take to shore up cybersecurity that addresses governance and risk management; business continuity and disaster recovery; server and workstation hardening; access control; application security; encryption; telecommunications, network security, and architecture; physical security of process control system equipment; service level agreements; operations security; education; and personnel security.

Partnerships

American Water has worked with several state and federal partners, and maintains a close partnership with the Department of Homeland Security to better understand new and emerging threats, and to validate and test its security controls. The company has also learned from previous threats, and conduct cybersecurity training and exercises to support continuous improvement. American Water actively attends classified briefings and shares intelligence and information in a two-way strategic partnership.

American Water also serves on the Water Information Sharing Analysis Center (ISAC) Board and participates at the Federal level as a member of the Water Sector Coordinating Council (WSCC) representing the National Association of Water Companies. In each of these partnerships, American Water analyzes and discusses with experts the latest threat information and specific response activities and strategies that are emerging in the sector.

American Water has identified these opportunities to collaborate:

1. **Communications and Teamwork**: encourage and direct more information sharing among utilities, emergency services, law enforcement, and the many other stakeholders that are active in the preparation for and reaction to Black Sky events and other disaster recovery efforts.
2. **Resiliency of Infrastructure and Assets**: support much-needed investment in the build-out of modern, resilient networks, which will be better able to respond to Black Sky events. This will include modernization of cost recovery mechanisms so that utilities will have the ability to devote resources necessary to bolstering networks and protecting consumers.
3. **Public-Private Partnerships:** support public-private partnership options to promote benefits of scale in the fight against cyberattacks and preparation for Black Sky events. Smaller public systems with limited resources are among the most vulnerable to these types of attacks. Leveraging the capacity of larger, more experienced and better-resourced utilities can help to ensure more robust security.
4. **Joint Black Sky Event Simulations:** call for and lead cross-sector Black Sky Day simulations that bring together state government, utilities, emergency services, law enforcement, and other stakeholders to develop and coordinate response strategies.

Conclusion

Much like the state government, American Water is focused on cybersecurity as the company continues to leverage a range of new technologies to benefit its customers. Ultimately, the many benefits of 21st century intelligent utility systems far outweigh any costs or risks that might arise from the threat of a Black Sky event. We have to remain vigilant and pro-active. The ultimate security and resiliency of our technology systems is dependent upon close collaborations with state and federal partners and industry.